

AMENDMENTS TO THE DRAWINGS

The attached sheet of drawings includes changes to Figure 3.

Figure 3 has been amended to include the legend "Conventional Art."

Attachment: Replacement sheet

REMARKS

Claims 1-6 are currently pending, wherein claims 1, 3, 4, and 6 have been amended to correct typographical errors. Applicants respectfully request favorable reconsideration in view of the remarks presented herein below.

At the outset, Applicants note with appreciation the indication that claims 3 and 6 contain allowable subject matter and would be allowed if rewritten in independent form.

In paragraph 1 of the Office Action ("Action"), the Examiner asserts that FIG. 3 should be designated by a legend such as Prior Art because only that which is old is illustrated. Applicants hereby amend FIG. 3 to include the legend conventional art as illustrated in the attached replacement sheet, thereby addressing the Examiner's concerns.

In paragraph 2 of the Action, the Examiner objects to claims 3 and 6 because it is allegedly unclear whether "the second...divided data packet" recited in claims 3 and 6 refers to the "plurality of divided data packets" or the "two or more associated divided packets." Applicants hereby amend claims 3 and 6, thereby addressing the Examiner's concerns.

In paragraph 4 of the Action, the Examiner rejects claims 1, 2, 4, and 5 under 35 U.S.C. § 103(a) as allegedly being unpatentable over U.S. Patent No. 5,113,392 to Takiyasu et al. ("Takiyasu") in view of U.S. Patent No. 5,161,189 to Bray et al. ("Bray"). Applicants respectfully traverse this rejection.

In order to support a rejection under 35 U.S.C. § 103, the Action must establish a *prima facie* case of obviousness. To establish a *prima facie* case of obviousness, three criteria must be met. First, there must be some motivation to combine the cited references. Second, there must be a reasonable expectation of success. Finally, the combination must teach each and every claimed element. In the present case, claims 1, 2, 4, and 5 are not rendered unpatentable by the combination of Takiyasu and Bray because the Examiner fails to establish a *prima facie* case of obviousness, as discussed below.

Independent claim 1 defines a cryptographic apparatus for encrypting packet data to be transmitted and received between terminals. The apparatus includes, *inter alia*, a plain text packet receiver for receiving packet data, a fragmentation determination unit that determinations whether there is a need for fragmentation of the packet data by computing the packet length when the packet data is encrypted and by comparing the computed packet length with a predetermined packet length, a fragmentation unit that divides, if needed, the packet data into a plurality of divided data groups and setting the divided data groups in a plurality of divided data packets of a predetermined data structure capable of being transmitted to and reconstructed in a transmission destination terminal by adding control information to each divided data packet for ensuring continuity between the divided data packets, an encryption unit for separately encrypting the plurality of divided data packets to form a plurality of encrypted packets, and an encrypted packet transmitting unit that transmits the plurality

of encrypted packets to a decryption terminal. In addition, the plurality of divided data packets include two or more associated divided data packets and the control information permits the associated divided data packets to be transmitted to the transmission destination terminal independently without waiting for the arrival of any other associated divided data packet.

Takiyasu discloses a communication apparatus capable of efficiently using buffer memory for storing received packets and reassembling them without discarding any received packets because of insufficient memory space. In addition, Takiyasu discloses that the communication apparatus can be used in a network where a source communication apparatus transmits a message to a destination communication apparatus in the form of fixed length packets, where the destination apparatus sequentially receives a plurality of packets from different source communication apparatus and reassembles them into messages. Although Takiyasu discloses dividing or fragmenting messages too large to be transmitted in a single fixed length packet into a plurality of message blocks, nowhere in Takiyasu is there any disclosure or suggestion of encrypting the packets prior to transmission or of determining the size of the packets after they are encrypted as claimed.

Bray discloses a method and apparatus for limiting the amount of bandwidth necessary to transmit an encrypted series of data packets by removing interleaved synchronization data between continuously transmitted messages and decrypting the message while properly synchronizing with the transmitted bits so no important data is

lost. More specifically, Bray discloses combining a data stream and the at least two message segments to be transmitted together into a single chained message. The chained message is then encrypted for example as shown in FIG. 5C. Although, Bray discloses encrypting a chained message such that any segment of the encrypted chained message may be independently decrypted, nowhere in Bray is there any disclosure or suggestion of separately encrypting a plurality of divided data packets to form a plurality of encrypted packets wherein the plurality of divided data packets include two or more associated divided data packets and control information that permits the associated divided data packets to be independently transmitted to a transmission destination terminal without waiting for the arrival of any other associated divided data packet as claimed. To the contrary, Bray specifically discloses encrypting the message segments as a single chained message.

In rejecting claim 1, the Examiner asserts that it would have been obvious to one skilled in the art to "provide encryption means to encrypt message segment[s] and decryption [sic] each message segment independently without waiting for the arrival of other segments," as allegedly taught by Bray in the system of Takiyasu in order to save time, energy and necessary RAM storage. To support this assertion, the Examiner points to column 2, lines 39-43 of Bray. This assertion is unfounded for the following reasons.

First, nowhere in Takiyasu is there any discussion of encrypting the data packets, or of the need or desire of encrypting the data packets. In addition, it is well known that

encrypting data packets increases the time and energy needed to transmit the packets. Therefore, one skilled in the art would not have been motivated to add encryption in order to save time, energy, and RAM storage as suggested by the Examiner because the system of Takiyasu does not utilize encryption.

Second, the method of Bray chains the message segments together before encrypting them whereas the system of Takiyasu is concerned with transmitting data packets in fixed length cells. Therefore, one skilled in the art would not have been motivated to add the chained message encryption method of Bray into the fixed length cell transmission system of Takiyasu. Accordingly, absent proper motivation to combine the teachings of Takiyasu and Bray, the rejection of claim 1 is improper.

Furthermore, even if, *arguendo*, one skilled in the art were motivated to combine Takiyasu and Bray, the combination would still fail to render claim 1 unpatentable because the combination of Takiyasu and Bray fails to disclose each and every claimed element.

Neither Takiyasu nor Bray disclose or suggest a cryptographic apparatus that includes a fragmentation determination unit that determines whether to note a data packet needs to be fragmenting into a plurality of dividing data packets by computing the packet length after packet is encrypted and comparing the computed packet length with a predetermined packet length, and a fragmentation unit that divides the packet data into a plurality of divided data groups and adds control information for ensuring continuity between the divided data packets as claimed. To the contrary, Takiyasu only

discloses dividing a packet data into a plurality of blocks based on the length of the data. Nowhere in Takiyasu is there any disclosure or discussion of encrypting the data packet or of determining the packet length after encryption. Although Bray discloses encrypting message segments, Bray discloses chaining the message segments together before encryption. Therefore, Bray cannot be interpreted as disclosing determining the packet length after encryption as claimed.

Since Takiyasu and Bray both fail to disclose or suggest a cryptographic apparatus that includes a fragmentation determination unit and a fragmentation unit as claimed, the combination of these two references cannot possibly disclose or suggest said elements. Therefore, even if one skilled in the art were motivated to combine Takiyasu and Bray, which Applicants do not concede, the combination would still fail to render claim 1 unpatentable because the combination fails to disclose each and every claimed element.

Claim 2 defines a cryptographic communication system that includes, in addition to the cryptographic apparatus of claim 1, a decryption apparatus that receives the plurality of encrypted packets from the cryptographic apparatus, separately decrypts each of the plurality of encrypted packets in the divided packets and transmits the plurality of divided data packets to a transmission destination terminal in same order they were decrypted.

Claim 2 is patentable over the combination of Takiyasu and Bray not only for those reasons presented above with respect to claim 1, but also because neither

Takiyasu nor Bray disclose or suggest a decryption apparatus that transmits the plurality of divided data packets to a transmission destination terminal in the same order in which they were decrypted.

Independent claims 4 and 5 define a cryptographic method that includes, *inter alia*, determining whether or not packet data needs to be fragmented by computing the packet length of the packet data after the packet data is encrypted and comparing the computed packet length with a predetermined packet length, and dividing the packet data into a plurality of divided data groups if fragmentation is needed and adding control information for ensuring continuity between the divided data packets. Accordingly, independent claims 4 and 5 are patentable over the combination of Takiyasu and Bray for at least those reasons presented above with respect to claims 1 and 2.

For at least those reasons presented above, Applicants respectfully request reconsideration and withdrawal of the rejection of claims 1, 2, 4, and 5 under 35 U.S.C. § 103(a).

The application is in condition for allowance. Notice of same is earnestly solicited. Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact Penny Caudle (Reg. No. 46,607) at the telephone number of the undersigned below, to conduct an interview in an effort to expedite prosecution in connection with the present application.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2448 for

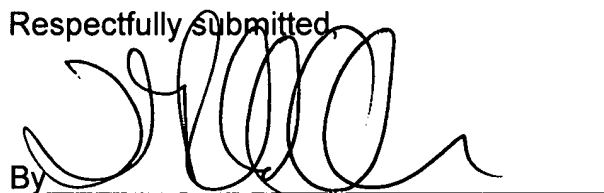
Application No. 09/898,024
Amendment dated June 29, 2006
Reply to Office Action of April 4, 2006

Docket No.: 0054-0236P

any additional fees required under 37 C.F.R. §§ 1.16 or 1.17; particularly, extension of time fees.

Dated: June 29, 2006

Respectfully submitted,



By _____
D. Richard Anderson
Registration No.: 40,439
BIRCH, STEWART, KOLASCH & BIRCH, LLP
8110 Gatehouse Road
Suite 100 East
P.O. Box 747
Falls Church, Virginia 22040-0747
(703) 205-8000
Attorney for Applicant

Attachment: Replacement Sheet of Drawings – Fig. 3